

What is claimed is:

1. A method for a secure transaction over a multi-computer network comprising the steps of:
 - a. providing at least two separate computer programs that are designed to communicate with each other over a multi-computer network, each separate computer program resident and runnable on a separate computer of the multi-computer network, at least one of the at least two separate computer programs further being a security server program for receiving and processing the secure transaction and at least one of the at least two separate computer programs further being a customer program;
 - b. running the security server program on a substantially continuous basis thereby making it available to receive secure transactions;
 - c. running the customer program on an as needed basis for communicating with the security server program with the customer program across a first communication port;
 - d. receiving a dynamically assigned port address from the security server program, further, receiving from the security server program a public set of numbers and a security server intermediate value that was calculated using at least the public set of numbers;
 - e. switching the customer program to the second port address for further communications with the security server program;
 - f. having the customer program calculate a customer intermediate value using at least the public set of numbers and a shared final value using at

- 23 least the customer intermediate value and the security server intermediate
 - 24 value;
 - 25 g. sending the customer intermediate value to the security server program;
 - 26 h. having the security server program calculate the shared final value using
 - 27 the customer intermediate value and the security server intermediate
 - 28 value;
 - 29 i. having both the security server program and the customer program create
 - 30 an encryption key using at least the shared final value;
 - 31 j. having the customer computer encrypt transaction information using the
 - 32 encryption key;
 - 33 k. sending the encrypted transaction information to the security server
 - 34 program;
 - 35 l. having the security server program de-crypt the encrypted transaction
 - 36 information; and
 - 37 m. having the security server program process the transaction.
-
- 1 2. The method according to claim 1 wherein the public set of numbers is at least a
 - 2 public prime number and a prime modulus number.
-
- 1 3. The method according to claim 2 wherein the customer intermediate value is
 - 2 further calculated using a customer selected random number and the security
 - 3 server intermediate value is calculated using a security server selected random
 - 4 number.

- 1 4. The method according to claim 3 wherein the shared final value is calculated by
2 the customer computer program using at least the security server intermediate
3 value, the customer selected random number, and the prime modulus; and the
4 shared final value is calculated by the security server program using at least the
5 customer intermediate value, the security server selected random number, and the
6 prime modulus.
- 1 5. The method according to claim 4 wherein the step of creating an encryption key
2 using at least the shared final value comprises at least the step of passing at least a
3 portion of the shared final value through a further encryption algorithm.
- 1 6. The method according to claim 5 wherein the further encryption algorithm is a
2 one-way function.
- 1 7. The method according the claim 1 further including the step of having the
2 customer computer program send customer profile information to the security
3 server program for comparison with customer profile information previously
4 stored on a computer memory accessibly by the security server program, thereby
5 verifying the identity of the customer.
- 1 8. The method according the claim 1 further including the step of having the
2 customer computer program send customer profile information to the security
3 server program for comparison with customer profile information previously
4 stored on a computer memory accessibly by the security server program, thereby
5 verifying the identity of the customer.

